Abstract of the Disclosure

Network intrusion detection accurately identifies and takes into consideration currently running network applications by examining machine instructions embodying those applications. Intrusion detection using application-specific intrusion criteria (e.g., normal communication behavior tracking criteria and/or intrusion signatures) allows application-specific responses to intrusions. Dynamic loading and checking for intrusion signatures may be performed by intrusion detection components that run in the same context as the running application being monitored. A central security authority may provide a repository for, and maintain, up to the minute intrusion signatures for networked machines. Application communications may be tracked to identify abnormal application behavior, and a network security administrator may be notified that a particular application may be making the network vulnerable to intrusion. Immediate response to abnormal application behavior or detection of an intrusion signature is made possible, while non-targeted applications on a targeted computing system may continue their network activity.